24

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/714,082	11/16/2000	Lewis T. Donzis	NORR0007US(12514RXUS02U)	5132

21906 7590 07/16/2004

TROP PRUNER & HU, PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
LAZARO, DAVID R	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/714,082	DONZIS ET AL.	
	Examiner	Art Unit	
	David Lazaro	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed 06/03/04.

2. Claims 8 and 31 were amended.

3. Claims 32-39 were added.

4. Claims 1-39 are pending in this Office Action.

5. The objections to Claims 8 and 31 are withdrawn.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-3, 6-8, 11-15, 18, 19, 21-23, 27, 28 and 30-39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,473,798 by Grosser, Jr. et al. (Grosser).

8. With respect to Claim 1, Grosser teaches a method of determining if a link is alive (Col. 1 lines 8-14), comprising: establishing a secure link (Col. 1 lines 33-55) between a first node (Col. 3 lines 22-33) and a second node (Col. 3 lines 46-49) according to a security protocol (Col. 4 lines 23-28); sending at least one ping message targeting the second node over the secure link (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60); and monitoring for at least one ping reply to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

9. With respect to Claim 2, Grosser teaches all the limitations of Claim 1 and further teaches establishing the secure link comprises establishing a virtual private network session (Col. 1 lines 33-41).

10. With respect to Claim 3, Grosser teaches all the limitations of Claim 1 and further teaches establishing the secure link comprises establishing a link protected by an Internet Protocol Security protocol (Col. 4 lines 23-28).

11. With respect to Claim 6, Grosser teaches all the limitations of Claim 1 and further teaches establishing the secure link comprises establishing the secure link between first and second nodes each comprising a security gateway (Col. 3 lines 23-28 and lines 34-39).

12. With respect to Claim 7, Grosser teaches all the limitations of Claim 6 and further teaches sending at least one ping message targeting another node behind the second node (Col 6 lines 37-51).

13. With respect to Claim 8, Grosser teaches all the limitations of Claim 7 and further teaches monitoring for at least one ping reply from the other node (Col. 6 line 61 – Col. 7 line 8).

14. With respect to Claim 11, Grosser teaches a method of communicating with a remote node (Col. 1 lines 8-14 and Col. 3 lines 46-49), comprising: establishing a secure link (Col. 1 lines 33-55 and Col. 4 lines 23-28) between a first security gateway (Col. 3 lines 23-28) and a second security gateway (Col. 3 lines 34-39), the remote node in communication with the second security gateway; sending at least one ping message to the remote node over the secure link and through the second security

gateway (Col. 6 lines 34-60); and monitoring for at least one ping reply from the remote node to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

15. With respect to Claim 12, Grosser teaches all the limitations of Claim 11 and further teaches establishing a secure link comprises establishing a secure link protected by an Internet Protocol Security protocol (Col. 4 lines 23-28).

16. With respect to Claim 13, Grosser teaches all the limitations of Claim 11 and further teaches establishing the secure link comprises establishing a virtual private network session (Col. 1 lines 33-41).

17. With respect to Claim 14, Grosser teaches all the limitations of Claim 11 and further teaches establishing the secure link comprises establishing a secure link protected according to a security protocol (Col. 4 lines 23-28).

18. With respect to Claim 15, Grosser teaches all the limitations of Claim 14 and further teaches sending the at least one ping message comprises sending at least one ping message defined outside the security protocol (Col. 6 lines 53-60).

19. With respect to Claim 18, Grosser teaches a system for communicating (Col. 1 lines 8-14) between a network element and a remote node (Col. 3 lines 46-49), comprising: a security module adapted to establish a secure link with the remote node, the secure link (Col. 1 lines 33-55), having a security mechanism according to a security protocol (Col. 4 lines 23-28); and a keep-alive module adapted to send at least one ping message over the secure link to the remote node (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60).

20. With respect to Claim 19, Grosser teaches all the limitations of Claim 18 and further teaches the security protocol comprises an Internet Protocol Security Protocol (Col. 4 lines 23-28).

21. With respect to Claim 21, Grosser teaches all the limitations of Claim 18 and further teaches an interface to a packet-based network, the secure link established over the packet-based network; and a layer to control communications over the packet-based network (Col. 1 lines 16-42 and lines 43-48).

22. With respect to Claim 22, Grosser teaches all the limitations of Claim 21 and further teaches the layer comprises an Internet Protocol layer (Col. 1 lines 16-21).

23. With respect to Claim 23, Grosser teaches all the limitations of Claim 18 and further teaches the keep-alive module is adapted to further monitor for at least one ping reply responsive to the at least one ping message to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

24. With respect to Claim 27, Grosser teaches an article comprising at least one storage medium containing instructions for controlling communications (Col. 7 lines 20-47), the instructions when executed causing a controller to: establish a secure link (Col. 1 lines 33-55) between a first node (Col. 3 lines 22-33) and a second node (Col. 3 lines 46-49) according to a security protocol (Col. 4 lines 23-28); send at least one ping message targeting the second node over the secure link (Col. 6 lines 34-60), the at least one ping message defined outside the security protocol (Col. 6 lines 53-60); and monitor for at least one ping reply to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

25. With respect to Claim 28, Grosser teaches all the limitations of Claim 27 and further teaches the instructions when executed cause the controller to further establish an Internet Protocol security association for the secure link (Col. 4 lines 23-28).

26. With respect to Claim 30, Grosser teaches all the limitations of Claim 27 and further teaches the controller is part of the first node (Col. 5 lines 24-28).

27. With respect to Claim 31, Grosser teaches a data signal embodied in a carrier wave and containing instructions for controlling communications (Col. 7 lines 20-47), the instructions when executed causing a system to : establish a secure link (Col. 1 lines 33-55 and Col. 4 lines 23-28) between a first security gateway (Col. 3 lines 23-28) and a second security gateway (Col. 3 lines 34-39), send at least one ping message to a remote node over the secure link and through the second security gateway (Col. 6 lines 34-60); and monitor for at least one ping reply from the remote node to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8).

28. With respect to Claim 32, Grosser teaches all the limitations of Claim 1 and further teaches sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

29. With respect to Claim 33, Grosser teaches all the limitations of Claim 1 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec as stated in Col. 4 lines 23-28).

30. With respect to Claim 34, Grosser teaches all the limitations of Claim 15 and further teaches sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

31. With respect to Claim 35, Grosser teaches all the limitations of Claim 15 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec as stated in Col. 4 lines 23-28).

32. With respect to Claim 36, Grosser teaches all the limitations of Claim 18 and further teaches sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

33. With respect to Claim 37, Grosser teaches all the limitations of Claim 18 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec as stated in Col. 4 lines 23-28).

34. With respect to Claim 38, Grosser teaches all the limitations of Claim 27 and further teaches sending the at least one ping message comprises sending the at least one ping message protected according to the security protocol (Col. 4 lines 23-28).

35. With respect to Claim 39, Grosser teaches all the limitations of Claim 27 and further teaches the security protocol comprises an Internet Protocol Security protocol (IPsec) (Col. 4 lines 23-38), and wherein sending the at least one ping message comprises sending the at least one ping message encrypted according to an IPsec security association (This would be inherent in the use of IPsec as stated in Col. 4 lines 23-28).

Claim Rejections - 35 USC § 103

36. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

37. Claims 4, 5, 16, 17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,182,226 by Reid et al. (Reid).

38. With respect to Claim 4, Grosser teaches all the limitations of Claim 3 but does not explicitly disclose sending a ping message comprising sending at least one Internet Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61).

39. With respect to Claim 5, Grosser teaches all the limitations of Claim 1 but does not explicitly disclose sending a ping message comprising sending at least one Internet Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61).

40. With respect to Claim 16, Grosser teaches all the limitations of Claim 15 but does not explicitly disclose sending a ping message comprising sending at least one Internet Control Message Protocol (ICMP) message. Reid teaches sending a ping message may comprise sending at least one ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the method disclosed by Grosser and modify it as indicated by Reid such that sending the at least one ping message comprises sending at least one Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61).

41. With respect to Claim 17, Grosser in view of Reid teaches all the limitations of Claim 16 and further teaches establishing a secure link comprises establishing a secure link according to an Internet Protocol Security protocol (Col. 4 lines 23-28 of Grosser).

42. With respect to Claim 20, Grosser teaches all the limitations of Claim 18 but does not explicitly disclose the ping message comprising an Internet Control Message Protocol (ICMP) message. Reid teaches a ping message may comprise a ICMP message (Col. 15 lines 59-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system disclosed by Grosser and modify it as indicated by Reid such that the at least one ping message comprises an Internet Control Message Protocol message. One would be motivated to have this since it is a "commonly known" way to send a ping message and could therefore be more easily incorporated into existing systems (Col. 15 lines 59-61).

43. Claims 9, 10, 24, 25 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,636,898 by Ludovici et al. (Ludovici).

44. With respect to Claim 9, Grosser teaches all the limitations of Claim 1. Although Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), Grosser does not explicitly disclose tearing down the secure link if it is determined to not be alive. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have

been obvious to one of ordinary skill in the art at the time the invention was made to take the method of Grosser and modify it as indicated by Ludovici such that the method further comprises tearing down the secure link if the secure link is determined not to be alive. One would be motivated to have this as it ensures the system is not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10).

45. With respect to Claim 10, Grosser in view of Ludovici teaches all the limitations of Claim 9 and further teaches tearing down the secure link comprises tearing down a security association according to an Internet Protocol Security protocol (Col. 1 lines 49-51 and Col. 5 lines 30-36 of Ludovici).

46. With respect to Claim 24, Grosser teaches all the limitations of Claim 23. Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), but does not explicitly disclose the security module being adapted to tear down a security association of a secure link if it is not alive. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link and its security associations (Col. 1 lines 49-51 and Col. 5 lines 30-36) should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system of Grosser and modify it as indicated by Ludovici such that the security module is adapted to tear down a security association of the secure link if the secure link is not alive. One would be motivated to have this as it ensures the system is

not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10).

47. With respect to Claim 25, Grosser in view of Ludovici teaches all the limitations of Claim 24 and further teaches the security association comprises an Internet Protocol Security protocol security association (Col. 1 lines 49-52 of Ludovici).

48. With respect to Claim 29, Grosser teaches all the limitations of Claim 28. Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), but does not explicitly disclose tearing down the security association if the controller does not receive the at least one ping reply. Ludovici teaches that in a VPN using a secure link, such as those using IPSec protocol (Col. 1 lines 49-52), the link and its security associations (Col. 1 lines 49-51 and Col. 5 lines 30-36) should be torn down when errors concerning the link are detected (Col. 1 line 57 – Col. 2 line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system of Grosser and modify it as indicated by Ludovici such that the instructions when executed cause the controller to tear down the security association if the controller does not receive the at least one ping reply. One would be motivated to have this as it ensures the system is not compromised and enables more efficient management of connection lifetimes and security associations (Col. 1 line 57 – Col. 2 line 10).

49. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Grosser in view of U.S. Patent 6,173,411 by Hirst et al. (Hirst). Grosser teaches all the

limitations of Claim 18 and further teaches the keep-alive module is adapted to further monitor for at least one ping reply responsive to the at least one ping message to determine if the secure link is alive (Col. 6 line 61 – Col. 7 line 8). Although Grosser teaches remedial action may occur to correct a link that is not alive (Col. 5 lines 9-12), Grosser does not explicitly disclose establishing a link over a secondary communication network if the secure link is not alive. However, Hirst teaches that upon detecting a link is not alive, one can establish a link over a secondary communication network (Col. 2 line 54 – Col. 3 line 13). It would have been obvious to one of ordinary skill in the art at the time the invention was made to take the system disclosed by Grosser and modify it as indicated by Hirst such that the system further comprises a module adapted to establish a link over a secondary communication network if the secure link is not alive. One would be motivated to have this since the reliability of a network connection is a critical concern (Col. 1 lines 20-35).

Response to Arguments

50. Applicant's arguments filed 06/03/2004 have been fully considered but they are not persuasive.

51. Applicants' Argue - "*The test packet sent in a Layer 2 tunnel as performed in Grosser does not constitute sending a ping message over a secure link as recited in claim 1. As expressly taught by Grosser, "the three Layer 2 tunnels discussed above do not themselves specify or provide data security." Grosser, 4:23-24. In other words, the Layer 2 tunnels described in Grosser are not secure links, and therefore, sending test*

packets in the Layer 2 tunnels to test the Layer 2 tunnels do not constitute sending a ping message over a secure link."

a. A "link" is defined by the Applicants' specification as referring to "one or more communication channels between two nodes" (Page 4 lines 31-32). In Grosser, all traffic will flow between the remote site client through the tunnel to the enterprise network server (Col. 3 lines 60-65 of Grosser). Thus, the communications from the remote site through the tunnel forms a link, since it acts as a communication channel between two nodes. A "secure link" is defined by the Applicants' specification as being "protected by a security mechanism" (Page 5 lines 1-2). While Applicant is correct in Grosser's statement of Layer 2 tunnels not providing security themselves, Grosser further states that "PPP or IPSec packet encryption can be utilized in conjunction with Layer 2 VPN tunneling to provide packet security at least between tunnel endpoints" (Col. 4 lines 23-28). As such, the examiner considers a Layer 2 VPN tunnel that is protected by a security mechanism such as IPSec packet encryption to be a "secure link." Therefore, Grosser does teach sending a ping message over a secure link as recited in Claim 1.

52. Applicants' argue - "*The Office Action cited column 1, lines 8-14, of Grosser as teaching the establishing of a secure link. The cited passage of Grosser describes virtual private networks (VPNs). However, note that the sending of test packets to test*

Layer 2 Tunnels as described by Grosser is not the same as sending test packets to test the VPNS."

b. The Examiner cites Col. 1 lines 8-14 of Grosser as teaching "determining if a link is alive", not establishing a secure link. Col. 1, lines 33-55 of Grosser is cited as teaching "establishing a secure link". As noted by Grosser, an essential part of a VPN is the ability to communicate with non-IP protocols over IP protocol networks (Col. 1 lines 43-56). Tunneling provides this functionality and can further provide a secure link when used in conjunction with a common encryption scheme (Col. 1 line 36-39) such as IPSec (Col. 4 lines 23-28). The claim language is directed towards "determining if a link is alive", not necessarily an entire VPN. As such, the examiner interprets Grosser as teaching a VPN can be made up of multiple secure links and presents a method of determining if a particular secure link is "alive".

53. Applicants' argue - "*...to test a tunnel (defined according to a Layer 2 protocol), a test packet according to the same Layer 2 protocol is sent through the Layer 2 tunnel. Therefore, the recitation in claim 1 that the ping message is defined outside the security protocol cannot be satisfied by Grosser.*"

c. The security protocol used by Grosser in one embodiment is IPSec as noted earlier (Col. 4 lines 23-48). The test packet as disclosed by Grosser is preferably defined by they type of Layer 2 tunnel utilized such as a L2TP Hello

for an L2TP tunnel, which is not IPSec. Therefore the ping message is defined outside the security protocol.

54. Applicants' argue - "*Grosser…does not disclose sending a ping message to a remote node over a secure link and through a security gateway, and monitoring for a ping reply from the remote node to determine if the secure link is a live…Grosser does not teach sending a ping message to a remote node through a security gateway….there is no indication that the test packet is sent through a security gateway….there is no indication that the gateway 24 is a security gateway.*"

d. The enterprise network server is also stated as being inside, behind or parallel to a firewall (a security gateway). If it is behind a firewall then the test packet will have to be sent through the firewall. The examiner interprets the cited Column 3, line 34-39 of Grosser as stating possible embodiments with concern to how the remote site is configure. One possible embodiment states the remote site "may also be implemented as a conventional LAN or WAN." As described in Col. 3 lines 18-33, the intranet 14 is described as a conventional LAN and includes a firewall. Thus, the examiner interprets a conventional LAN to include a firewall and therefore remote site 16 would have a firewall (security gateway) through which any test packet would have to be sent. In general, Grosser implies that there are many possible configurations for either network site as would be expected in a typical local to remote networking environment. Furthermore, the NAC at remote site 16 could also be considered a "security

gateway" since it performs authentication of the client trying to establish the tunnel to the ENS 28 (Col. 3 lines 47-64).

55. Applicants argue - "*Applicant respectfully submits that there is absolutely no need for use of an ICMP messages as a ping message in Grosser…Moreover, using the ICMP message to test the Layer 2 tunnel of Grosser would render the Grosser test inoperative for its intended purpose. Sending an ICMP message through a Layer 2 tunnel would not enable testing of the Layer 2 tunnel, since ICMP is a message defined by a higher level protocol.*"

e. Grosser broadly teaches a "test packet" (Col. 6 lines 50-52), and the examiner interprets this "test packet" to be a type of ping. While Grosser presents a preferred embodiment of using a ping defined by the type of tunnel, Grosser does not explicitly limit the protocol used for the ping. The Examiner's rejection suggests ICMP was available to form the ping message. Furthermore, the mere fact that ICMP originates from a higher layer does not render the test inoperative. Wrapping and encapsulation provides the mechanism for communication between the layers of the endpoints. As such, an ICMP ping message can be encapsulated and sent to the second node of the secure link where the ping message will be extracted and acted upon. If there is no response, one could still assume a problem with the tunnel or the second node. This is the basic concept taught by Grosser in determining responsiveness of the secure link (Col. 6 lines 50-65).

Conclusion

56. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Lazaro whose telephone number is 703-305-4868. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain Alam can be reached on 703-308-6662. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

David Lazaro
July 14, 2004

HOSAIN ALAM
SUPERVISORY PATENT EXAMINER